CSC-EPL-88 008

(2)

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF INFOSAFE CORPORATION

X-LOCK 50

VERSION 2.00

12 September 1988

91 4

SUBSYSTEM EVALUATION REPORT

INFOSAFE CORPORATION

X-LOCK 50 VERSION 2.0

NATIONAL COMPUTER SECURITY CENTER

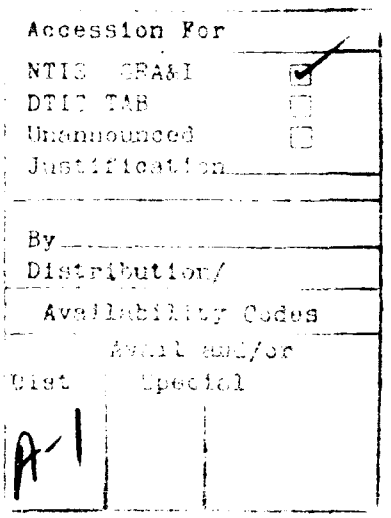
9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

September 12, 1988

Library No. S231,326

FOREWORD

This publication, the Subsystem Evaluation Report of InfoSafe Corporation's X-LOCK 50 Version 2.0, is issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." This report documents the results of an evaluation of InfoSafe's product X-LOCK 50 Version 2.0. The requirements stated in this report are taken from *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA* dated December 1985.



Approved:

September 12, 1988

Eliot Sohmer
Chief, Evaluations, Publications, and Support
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

Stephen D. Schneider

Richard A. Humphreys

Scott F. Korthals

Jose A. Rivera

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

Table of Contents

EXECUTIVE SUMMARY

X-LOCK 50 Version 2.0, has been evaluated by the National Computer Security Center (NCSC). X-LOCK 50 is considered to be a security subsystem rather than a complete trusted computer system. Therefore it was evaluated against a relevant subset of the requirements from the *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA* (Criteria), dated December 1985. The features included in this evaluation were Identification and Authentication (I&A), a limited form of Discretionary Access Control (DAC), and a limited form of Object Reuse (OR).

The NCSC evaluation team has determined that X-LOCK 50, when configured as tested, is capable of applying these security features on an IBM PC/XT or PC/AT.[1] I&A is maintained on the protected computer by requiring that users enter a valid user identification (ID) and password prior to gaining access to the system. The discretionary access control is implemented on a limited scale by allowing or denying an individual user access to the system or hard disk. Privileges assigned to users are determined by the superuser, (the system security administrator) when user accounts are being established. Object reuse, which is implemented at the user's discretion, only writes over specified files and does not take into consideration other locations (e.g., memory buffers) which could contain residual data. *Object reuse implemented in this manner does not meet the* DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA.

Encryption forms a significant part of the security of this system and the evaluation did verify that encryption took place. However, the method and effectiveness of the encryption was not evaluated. Encryption on the X-LOCK 50 set by the superuser, can either encrypt all files automatically or encrypt only files indicated by the individual user. If all files are automatically encrypted using the system master key, any user can still opt to have a file encrypted on a key different than the rest of the system. There is also an external cover lock which provides some security for the system's internal components.

These security mechanisms can be maintained only if the X-LOCK 50's hardware remains protected from physical tampering. If encryption is not used information can be taken from the hard disk after removal of the XLOCK 50 card or by directly addressing the hard drive from the floppy drive using a disk driver program.

Subsystems are not capable of protecting information with such assurance that classified information may be maintained on a system protected only by subsystems. Neither may subsystems be used to

---

1 IBM PC/AT and PC/XT are registered trademarks of the IBM Corporation.

upgrade the protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. XLock 50 is not capable of protecting information with such assurance that classified information may be maintained on a system protected only by XLock 50. Neither may XLock 50 be used to upgrade the protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. XLock 50 may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

Subsystems considered in the program are special-purpose products that can be added to existing computer systems to increase security and implement a security feature from the TCSEC, as well as have the potential of meeting the needs of both civilian and government departments and agencies.

For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem and the attached system, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an assessment is made of a subsystem's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

X-LOCK 50 is an integrated software/hardware security product which, when implemented on an IBM PC/XT/AT and configured as tested, provides user Identification and Authentication (I&A), a limited form of Discretionary Access Control (DAC), and a limited form of Object Reuse (OR). For a user to enter the system, he must first supply an ID and then a password for authentication. The access control is implemented by the superuser (a system administrator) and either allows or disallows a user access to the hard drive or the system. In addition the super user can specify whether or not general users will be allowed to boot the system from the floppy drive. Object Reuse on files is user discretionary while encryption can either be user implemented or automatically system implemented. X-LOCK 50 also includes an external cover lock to provide some physical security for the microcomputer's internal components.

The X-LOCK 50 package contains a plug-in card which occupies one of the microcomputer expansion slots, support software, and an external cover lock. The expansion card includes the firmware which controls access to the computer and its disk drive resources. This card also includes the necessary hardware for performing encryption and for storage of account and system information. The support software provides programs which perform account management, file encryption, secure information erasure and other functions. The support software requires that the operating system be MS-DOS V2.0 or higher.[1] The cover lock fits over one of the rear mounting screws, thus preventing access to the computer internals without the proper key. Although it would not take much effort to break the lock, the evidence of a break-in would be clear to the user.

Encryption is an integral part of the X-LOCK 50. However, it is important to realize that the method used to encrypt the data was not evaluated. The scope of the encryption evaluation only verified that the data in question actually appeared in some way transformed from the original input.

---

1 MS-DOS is a registered trademark of Microsoft Corporation.

Evaluation of Functionality

Identification and Authentication (I&A)

Before giving access to a computer system, X-LOCK 50 prompts each user for a valid ID and a corresponding password. As delivered there is no minimum ID or password length, however, a superuser can specify a minimum length. ID's and passwords have a maximum length of sixteen characters. User ID's and passwords are alphanumeric with no distinction between upper and lower case letters. Initially, the superuser assigns each user a unique ID and password. Subsequently, the users can select their own passwords. The superuser has the ability to force any or all users to change their passwords by "expiring" them. In this case the superuser does not see the actual passwords. He can also choose to change any user's password in which case he will obviously see and know the new password. X-LOCK 50 supports a maximum of 130 users.

User ID's, passwords and account information are encrypted and stored on the X-LOCK 50 plug-in card inside the computer's case. This information can also be stored in a backup file on the hard disk or on a system administrator diskette, which should be mantained and protected by the superuser. The superuser uses this diskette to establish and change user ID's, passwords and account information. When a user enters his own password at logon, it is transformed, encrypted and compared to the encrypted form stored in the memory chip. During the I&A process, the X-LOCK 50 identifies to itself the primary super user, other superusers and general users. The X-LOCK 50 logon procedure waits until the ID and password are both entered before any action is taken. Both data points must be valid and both must be related before access to the system is granted. Only superusers are authorized to create or delete user accounts or set/reset superuser status.

Additionally, the X-LOCK 50 has a system-lock penalty to inhibit the guessing of passwords. After the maximum number of unsuccessful attempts to enter a correct ID/password combination, X-LOCK 50 locks the system so that a cold boot is necessary to return to the regular logon procedure. The maximum number of allowable unsuccessful logons before lock-out is a figure that is set by the superuser (between 1-30 attempts).

Discretionary Access Control (DAC)

The X-LOCK 50 system provides discretionary access control to govern access to the hard disk and/or to the PC system itself. Also floppy drive boot capability can be allowed or denied to all general users. The superuser can define time periods during which a general user may log in to the system. When the user has successfully logged onto the system, he has access to all the standard system calls, in other words, complete control. However, X-LOCK 50 allows users to encrypt and hide their files from other users. Files hidden in this manner are not visible to the user using standard

system calls. The DAC mechanisms used by X-LOCK 50 meet the C1 level requirments of the *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA*.

The X-LOCK 50 card has a non-volatile RAM memory chip on board with which it stores tables of access control information. This information can be backed up onto hard disk or floppy disk for ease of administration (the backup file will be encrypted before creation). The User Account table contains the user ID's, passwords, user type and status of passwords. Also, this table stores a flag indicating whether or not the user floppy disk will always be encrypted. For general users this memory space is also used to keep the account access schedule (information about the times and days users have access to the system) and status of the hard disk and system access. Finally, a last table which is maintained in memory during the session of each user, contains the floppy encryption mode for that particular user and the user key.

X-LOCK 50 provides the general user with utility programs to perform the following functions: check account status, do password management, check security policy status, and encrypt/lock/decrypt individual files. The superuser can set a flag that causes the floppy disk to always be encrypted. If this flag is not set, the user has the choice to encrypt or decrypt any of his floppy disks. The user is allowed to use either the master or his own key for encryption and decryption. The use of the "master floppy key" is a way of allowing group access to all users of the computer.

A superuser has the ability to create or delete accounts, set/change passwords, set/reset superuser status, define some security policies and perform system maintenance. Additionally he can set/reset the floppy drive auto-encryption mode for individual users. The primary superuser password and the status of the primary superuser cannot be changed by any superuser. The primary superuser has access to run the hard disk encryption program and change the hard and floppy disk master encryption keys. These functions are privileged primary superuser options.

Access control policies, system access, and account maintenance are defined and executed by the superuser through the XUTIL50 program provided by X-LOCK 50. The XUTIL50 is a menu driven program that allows the superuser to edit user accounts, define the security policies, perform system maintenance and set the floppy encryption mode (depending on each type of user).

Object Reuse

X-LOCK 50 attempts to implement object reuse by means of a program called SCRUB. This program does object reuse in the sense that it overwrites the file, provided as a parameter to the program, with a bit pattern and deletes the pointer from the directory table. This program is user discretionary because X-LOCK 50 does not automatically enforce use of SCRUB. The user can still use the delete or erase file commands provided by the PC's operating system, although these don't provide object reuse.

A feature in the hard disk encryption program that encrypts the hard disk with SCRUB before data write, provides another protection against data scavenging. That is, each time a user opens an existing file to write into it, X-LOCK 50 will 'scrub' the hard disk space used by the old file version and then will encrypt and write the new file version, even if only changes were made to the old file. For application programs (e.g., editors and word processors) where backup files are created, X-LOCK 50 will not operate over those backup files. Even if the application program deletes the backup file, the data will still be in the disk space used by the backup file and can be reached using any disk search utility.

X-LOCK 50 does not modify the user's data work space after he logs off. Residual information in the transitive memory such as RAM and cache is not changed between user sessions. This lack of object reuse causes the X-LOCK 50 to fail the object reuse requirement of the *DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA*.

Evaluation of Documentation

All technical information relating to the X-LOCK 50 PC security system was obtained either through discussion with its designers, by review of the product documentation, or by testing. The X-LOCK 50 documentation package consists of one document, the X-LOCK 50 Operations Manual (copyright 1987). This 72 page document is intended for use by all X-LOCK 50 users. Described below, it contains a complete and detailed look at all the security features of X-LOCK 50. The documentation was found to be complete and accurate. It assumes that the superuser has reviewed the PC's "Guide to Operations" and the "Disk Operating System User's Guide" before attempting to use X-LOCK 50.

X-LOCK 50 Operations Manual

Chapter 1: Overview of X-LOCK 50

This chapter provides a general overview of the product. It briefly explains what X-LOCK 50 is, what it does, who can use it, and why security is important in today's computer-dependent society.

Chapter 2: Installation

This chapter provides step-by-step installation procedures for the X-LOCK 50 hardware and software.

Chapter 3: The Super User

Chapter 3 defines the responsibilities of a superuser. It explains the importance of the X-LOCK 50 security options and gives examples of how the options can be used in different environments. It also describes the issues and options associated with establishing and maintaining user accounts.

Chapter 4: General Users

This chapter explains the capabilities and limitations of general users. Included are options on changing passwords, encrypting/decrypting files and floppy disks, and examining account information.

Chapter 5: The XUTIL50 Program

Chapter 5 provides a detailed description of the XUTIL50 program, and explanations on the execution of its various functions. XUTIL50 includes the following functions:

a Edit user accounts

b. Define security policy

c. Perform system maintenance

d. Set floppy encryption mode

Chapter 6: The HDCRYPT Program

Chapter 6 provides a detailed description of the HDCRYPT program which is used to activate or deactivate system-level hard disk encryption. This chapter covers encrypting and decrypting the hard disk(s), and the various test and recovery features of the program.

Chapter 7: The XFILE50 Program

Discussed in this chapter is the XFILE50 program and how to encrypt or decrypt individual files.

Chapter 8: X-LOCK 50 Utility Programs

This chapter discusses several utility programs provided with the X-LOCK 50. These programs are:

SCRUB: implements object reuse. SCRUB first fills the chosen file with a series of patterns and then deletes the file.

LOGOFF: provides a means by which a user may log in to another account without rebooting his machine.

SETTIME: updates the DOS date and time to reflect the value in the X-LOCK 50 protected clock/calendar.

READTIME: displays the current date, day of the week, and time from the protected clock/calendar.

WHOAMI: displays the privilege level and account name of the currently logged in user and the system name.

Chapter 9: Warranty

Warranty and FCC Compliance information is discussed in this chapter.

Chapter 10: Glossary

This chapter contains a Glossary of Terms.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data stored on these systems. Initially, protection was provided solely by the individual who maintained physical possession of his own data and operating system on diskettes, resulting in a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and users' data. Other security mechanisms were not deemed necessary since the user was only able to inflict damage to his own data or operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In a working environment where it was common to have many users share the same workstation, they now shared and stored their data on the same hard disk drive unit. In this environment, users no longer had the assurance that their data was protected from unauthorized access, or even that the underlying operating system had not been subverted. Procedural controls could no longer provide the adequate user isolation and controlled sharing necessary for this environment.

X-LOCK 50 is designed to add assurance in the protection of the shared workstation. When configured as tested, X-LOCK 50 provides identification & authentication, and automatic encryption. X-LOCK 50 also provides a limited amount of discretionary access control (DAC).

The identification & authentication mechanism allows control over who uses the workstation. This is accomplished by requiring a user to enter two data points, both an identifier and a password. Having this mechanism implemented in hardware rather than software allows it to function effectively on a one state machine such as the IBM-PC/XT/AT.

Automatic encryption provides a method of protecting data from being read by personnel using the same machine but not authorized access to all data on that machine.

X-LOCK 50 provides some Resource Access Control in that the superuser may limit use of the hard disk or the computer as a whole. This is not as finely grained DAC as is traditionally associated with DAC over individual files. Additionally, X-LOCK 50 can prevent users from booting off of the floppy disk. This prevents the running of an operating system other than the one X-LOCK 50 was originally set up on.

Object reuse is implemented by allowing a user to dispose of a file by first clearing the information in it, and then releasing it back to the system.

PRODUCT TESTING

Test Procedure

Testing makes up a large portion of a subsystem evaluation. The testing performed was divided into two catagories: functional and security testing. The major features tested were Identification and Authentication (I&A), and a limited form of Discretionary Access Control (DAC). In addition to these major features, testing was also conducted on object reuse and file locking.

The functional testing was conducted to verify vendor claims about system capabilities. This included following all documented instructions concerning installation and initialization procedures. A superuser and several general users were created, and all commands available to each were tested.

The security testing was done to determine if system features could be subverted by a general user. Security testing included attempts at obtaining access to the system without I&A mechanisms being used, and acquiring access to resources denied by DAC. The methods of attack made use of DOS commands, utility programs which make BIOS calls, and the use of user device drivers. The attack also included attempts to reset all the interrupts to the values that existed prior to installation of the X-LOCK 50 card. Finally, an attempt was made to write to the hardware card's RAM address space.

All tests were performed on an IBM PC/XT/AT. The hardware included a monochrome monitor, and a floppy and hard disk drive. The software consisted of MS-DOS 3.3 operating system.[1]

Test Results

Identification and Authentication

Testing of the I&A mechanism showed that the system did not allow a user to gain access without first being identified and authenticated. It should be noted that another hardware card, if intialized prior to the X-LOCK 50 card, could give control back to DOS before I&A has taken place. Therefore, following the installation instructions and placing the X-LOCK 50 card in the first polled slot is important in maintaining system integrity. An attempt to read the hardware card's RAM memory with a utility program proved to be ineffective in obtaining any information necessary to bypass the I&A mechanism. However, parts of the hardware card's ROM memory could be read

---

1 MS-DOS is a registered trademark of Microsoft Corporation.

with a utility program. This allows a user to read certain ROM programs on the hardware card which may allow reverse engineering. It was also found that the authentication storage mechanism took a given password and compressed it to save storage space. This has the side effect of allowing two or more different passwords to be stored identically. This password compression technique will reduce the number of unique passwords by an insignificant amount. This was deemed to have a negligible effect on the security of the system.

Discretionary Access Control (DAC)

DAC testing was accomplished by attempting to gain access to objects beyond a specific user's access rights. The testers attempted to gain illegal access to a hard disk drive, the system itself, and superuser status. In addition attempts were made to boot from a floppy disk in order to bypass the X-LOCK 50 card. X-LOCK 50 was successfull in preventing any breach of security except in the protection of the hard disk. In the face of a determined attempt, when the user knows how to write or use a device driver program, X-LOCK 50 is unable to prevent access to the hard disk. However, if the encryption option (always encrypt floppy) is used and the system is configured as recommended, a user can not introduce a device driver into the system. The other three DAC mechanisms were not broken by any of the tests conducted.

Object Reuse:

X-LOCK 50 provides the user with a program to do object reuse. This program was tested by creating a file of information on the hard disk and running the object reuse program on it. The file was then viewed using a utility program . This showed that the file space was totally written over by "0"s. No residual information remained. As noted earlier, word processors with automatic back-up defeat this system of object reuse.

Encryption and File Locking:

X-LOCK 50 provides three different mechanisms of encryption that can be set or reset depending on the user type and encryption mode needed. The primary superuser can provide automatic encryption of the hard disk through the HDCRYPT program. All superusers can set the auto-encrypt mode of the floppy drive for individual users using the XUTIL50 menu driven program. (Once auto-encrypt is set it can not be reset by the general user.) The general user can set the automatic floppy drive encryption mode through the XUTIL50 program (if the superuser has not set this mode previously). He can use either a user defined key or the floppy disk master encryption key each time he logs onto the PC system. This mechanism of using the master floppy key for floppy drive encryption is useful, but allows all users on the system access. On the other hand using a personal key to encrypt the floppy disk will prevent any user from decrypting the floppy disk when using the master floppy key.

Another encryption mode allowing the user to enter a key which can be used to encrypt individual files is provided. This method is implemented in the XFILE50 program and can be used in either the hard disk or the floppy disk at any moment. In addition to the encryption, XFILE50 hides the file from a "dir" command in DOS. However, the hidden file can be found by the use of a utility program. The encryption program can also reverse the process for files under the entered "key".

The strength of this encryption was not tested, but is described as using the DES encryption algorithm.

Physical Security

X-LOCK 50 includes a lock which attaches to one of the screws that holds the cover on. This mechanism may not prevent determined entry, but it would provide an indication of whether the system has been tampered with.

Conclusions

X-LOCK 50 is a useful product for providing enhanced security to desktop IBM-compatible computers. Its greatest strength is its I&A mechanism. A determined, skillful authorized user can by-pass DAC unless floppy boots are prohibited, fullencryption is mandatory, and compilers/assembler and utilities that make BIOS calls are not put on the system. With these restrictions, Xlock 50 provides not just I&A but effective DAC. As long as physical security is maintained, the security mechanisms were effective (subject to the limitations noted in this report.)

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT UNLIMITED DISTRIBUTION
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL 88/008	5 MONITORING ORGANIZATION REPORT NUMBER(S) S231326
6a NAME OF PERFORMING ORGANIZATION National Computer Security Center	6b OFFICE SYMBOL (If applicable) C12
6c ADDRESS (City, State and ZIP Code) Ft. George G. Meade, MD 20755-6000	7a NAME OF MONITORING ORGANIZATION 7b ADDRESS (City, State and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)
8c ADDRESS (City, State and ZIP Code)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
	10 SOURCE OF FUNDING NOS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT NO
11 TITLE (Include Security Classification) EVALUATION REPORT: INFOSAFE CORPORATION X-LOCK 50 VERSION 2	
12 PERSONAL AUTHOR(S) Schneider, Stephen; Humphreys, Richard; Korthals, Scott; Riveria, Jose	
13a TYPE OF REPORT Final	13b TIME COVERED FROM TO
14 DATE OF REPORT (Yr, Mo., Day) 880912	15 PAGE COUNT 22
16 SUPPLEMENTARY NOTATION	
17 COSATI CODES FIELD / GROUP / SUB-GR	18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) NCSC TCSEC I&A DAC OR INFOSAFE X-LOCK 50

19 ABSTRACT (Continue on reverse side if necessary and identify by block number)

X-LOCK 50 Version 2.00, has been evaluated by the National Computer Security Center (NCSC). X-LOCK 50 is considered to be a security subsystem rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements from the ***DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA*** (Criteria), dated December 1985. The features included in this evaluation were Identification and Authentication (I&A), a limited form of Discretionary Access Control (DAC), and a limited form of Object Reuse (OR).

This report documents the findings of the evaluation.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL DENNIS E. SIRBAUGH	22b TELEPHONE NUMBER (Include Area Code) (301)859-4458 / 22c OFFICE SYMBOL C12

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE